ESERCIZIO DEL GIORNO – PRATICA S6/L3

TRACCIA: Scrivere un programma in Python che simuli un UDP flood, ovvero l'invio massivo di richieste UDP verso una macchina target che è in ascolto su una porta UDP casuale.

REQUISITI DEL PROGRAMMA:

Input dell'IP Target: Il programma deve richiedere all'utente di inserire l'IP della macchina target.

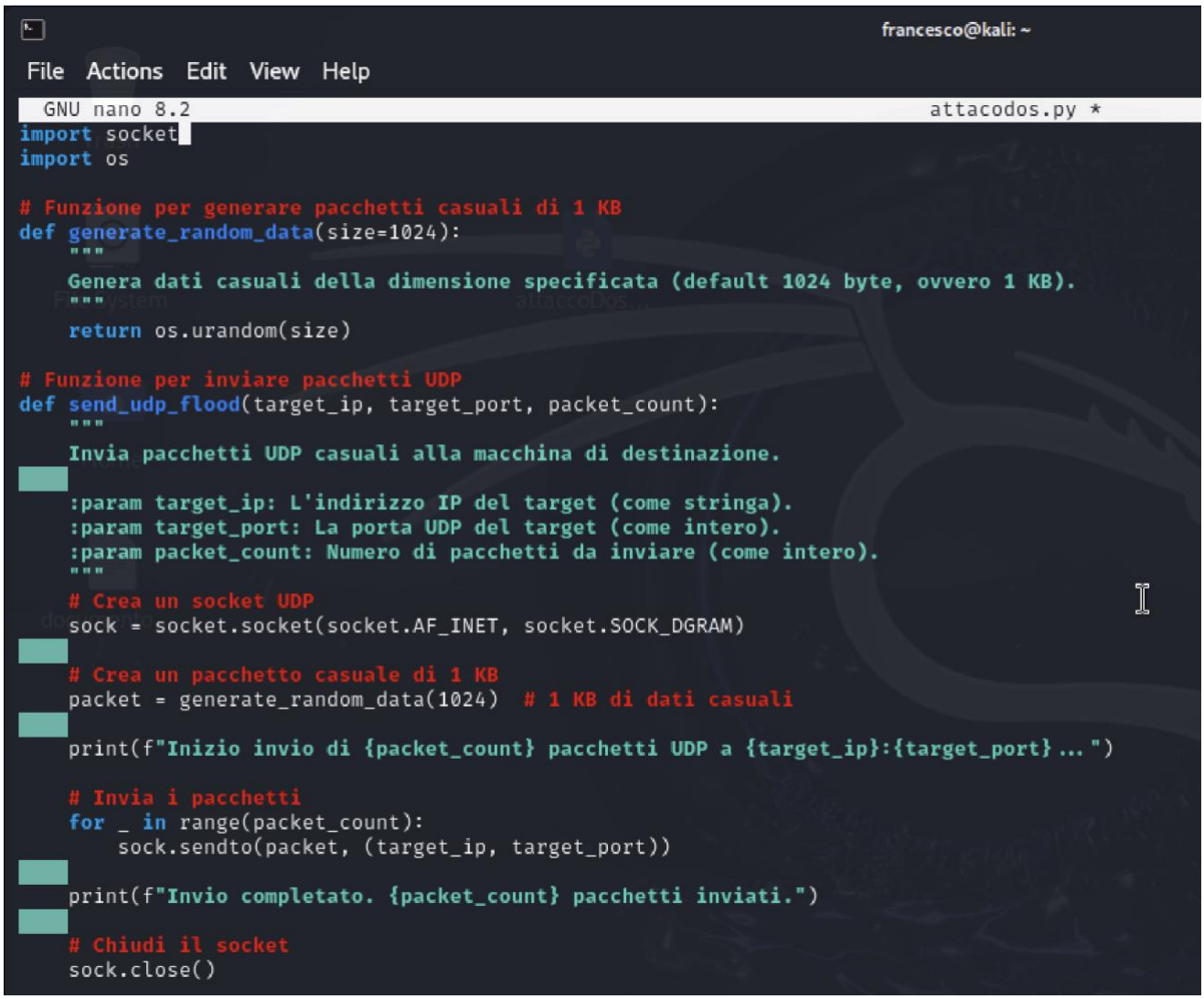
Input della Porta Target: Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.

Costruzione del Pacchetto: La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.

Suggerimento: per costruire il pacchetto da 1 KB, potete utilizzare il modulo random per la generazione di byte casuali.

Numero di Pacchetti da Inviare: Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

SCRITTURA DEL CODICE PYTHON:



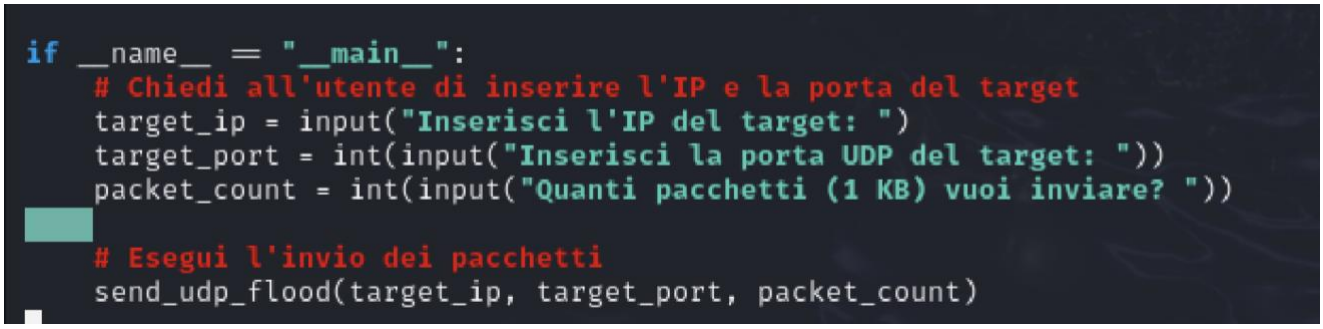
Analisi del codice:

Utilizziamo import **socket** e import **os**: la **prima** libreria è necessaria per la comunicazione di rete in python, la utilizziamo per creare un **socket UDP** e per inviare pacchetti di dati.
La seconda libreria **os** viene utilizzata per interagire con il sistema operativo, in questo caso per generare dati casuali (os.urandom).

Generate_random_data(size=1024): è la funzione che genera dati casuali di una determinata dimensione.

Os.random(size): utilizziamo os.random per ottenere size byte di dati casuali.
La funzione è stata impostata per generare 1024byte di dati (1KB).

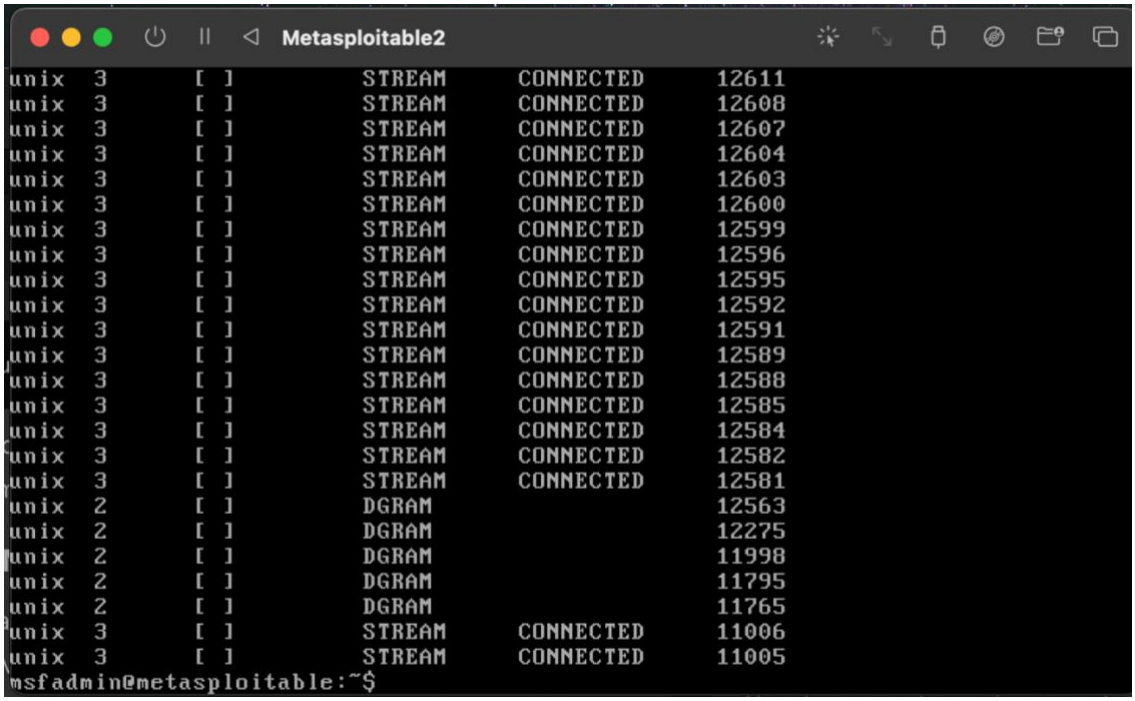
Funzione send_udp_flood (target_ip, target_port, packet_count):
Come si può intuire, questa funzione **invia** una serie di **pacchetti udp** casuali a una macchina di destinazione, il target ip, target port e packet count sono dati chiesti all'utente.



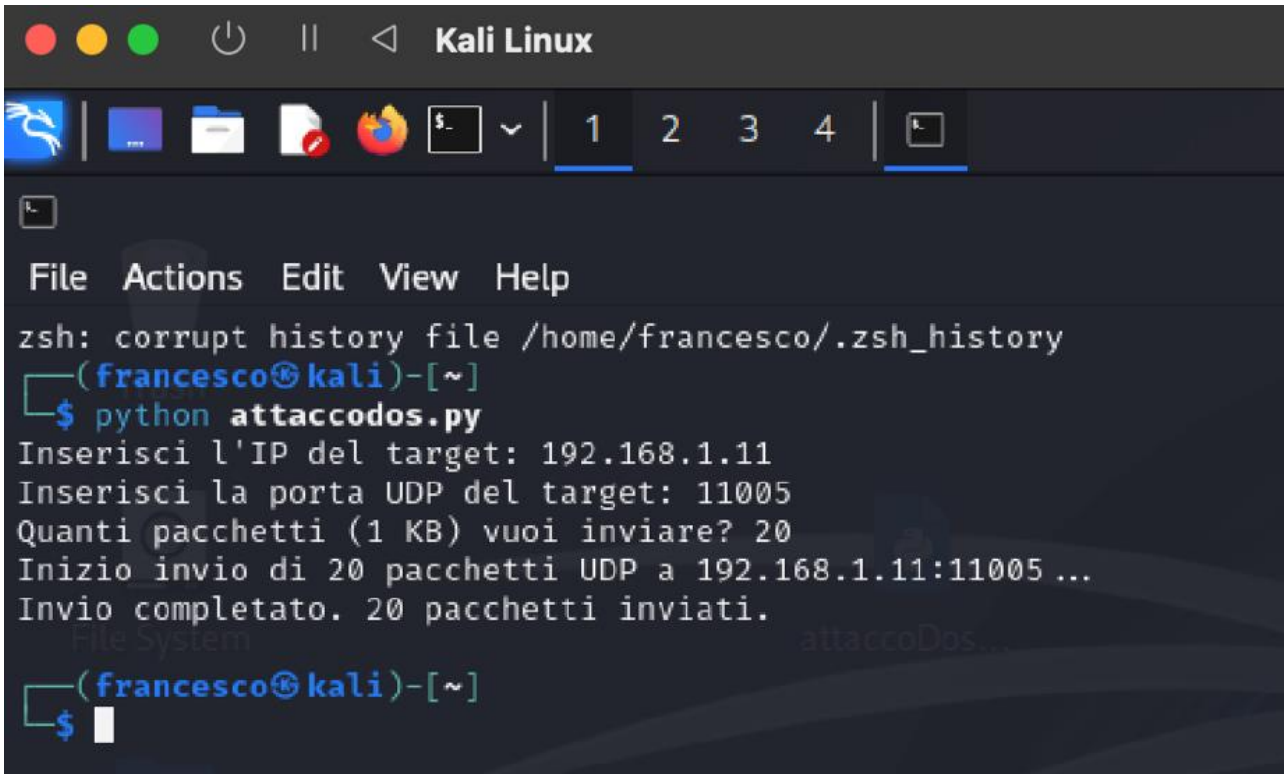
Una volta concluso il codice e verificato che non ci siano errori, possiamo fare una prova di funzionamento utilizzando come target la VM Metasploitable.

Il programma ci chiederà l'IP del target, il numero della porta ed il numero di pacchetti da inviare.
Quindi apro metasploitable e per essere sicuri utilizzo **ifconfig** per l'indirizzo IP e il comando **netstat -anu** (dove **-a**: Mostra tutte le connessioni e le porte in ascolto.
-n: Mostra gli indirizzi IP e le porte numeriche invece dei nomi simbolici.
-u: Limita la ricerca alle porte UDP.)

Questo comando, quindi, mostrerà un elenco delle porte UDP attualmente in ascolto su Metasploitable.



Scelgo una porta come target e proseguo con l'esecuzione del programma su Kali Linux.



Come possiamo vedere, il programma sembra funzionare correttamente.
Per prima cosa chiede all'utente di inserire l'IP del target, la porta UDP ed il numero dei pacchetti che vogliamo inviare.
Alla fine mostra anche un messaggio con scritto invio completato ed accanto il numero di pacchetti inviati.